



U.S. Department of Justice

Executive Office for United States Attorneys

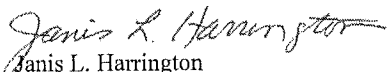
Acquisitions Staff

Suite 5200, Bicentennial Building
600 E Street, NW
Washington, DC 20530

(202) 616-6425
FAX (202) 616-6651

Date: February 24, 2010

To: All Contracting Officers
All Administrative Officers
All District Office Security Managers
All Civil Chiefs
All Criminal Chiefs
All First Assistant United States Attorneys

From: 
Janis L. Harrington
Assistant Director

Subject: Temporary Waiver of Security Clauses

The Executive Office for United States Attorneys (EOUSA) has obtained a limited twelve-month waiver from the provisions of DOJ Procurement Guidance Document 08-04 that sets forth required security clauses governing the use of computers by DOJ contractors who handle DOJ data, including personally identifiable information (PII). This waiver will allow us to continue to analyze the impact and application of these clauses. The waiver expires on February 16, 2011.

As you know, compliance with some of the provisions of the security clauses has been problematic for some contractors doing business with the United States Attorneys' Offices (USAO). The most common type of contract issued by the USAOs is for expert witness and litigative consultants – typically medical professionals, language experts, and experts in particular technologies or sciences. In many cases, these experts are self-employed, or have a small staff, may not be technologically savvy or have no “in-house” IT employees to enable compliance with these clauses.

This waiver applies only to contractors, to include Litigative Consultants and Expert Witnesses, who handle electronically stored information (ESI) containing the PII of 25 or fewer individuals in connection with services related to a specific case, claim, or investigation. These contractors are, however, required to certify compliance with the following security measures to safeguard the PII from loss or theft when using their own computers. The below requirements must be included in applicable contracts and are attached to this memorandum for use by Contracting Officers.

a. Systems Security:

1. Keep the computer in a safe place, such as a locked office or other location with limited access, when not in use.
2. Mark any laptop with contact information in case of loss to facilitate its safe return.
3. Keep the operating system, security and application software used in connection with any computer updated on a regular basis.
4. Use anti-viral software and a host-based firewall mechanism.

b. Data Security:

Notify the primary or alternate contact with the USAO as soon as possible, but in no event more than 24 hours after discovery, of the loss of any computer or PII covered under the contract.

c. Personally Identifiable Information Notification

Notification to any individual whose personally identifiable information was, or is reasonably believed to have been, breached will be the responsibility of the Executive Office for United States Attorneys, consistent with the Department's Data Breach Notification Procedures.

d. Pass-through of Security Requirements to Subcontractors

The requirements set forth in paragraphs a. through c. above, also apply to all subcontractors who perform work in connection with this contract.

Furthermore, due to the limited resources of these contractors, the time for notification of loss of PII in paragraph b. was extended to 24 hours. The USAOs will remain responsible for reporting the loss to the EOUSA Security Operations Center (803-705-5533) within one hour of being notified by the contractor. EOUSA will retain responsibility for notifying those individuals whose PII was lost by the contractor.

This temporary waiver will enable EOUSA, in concert with the Civil Chiefs' Working Group, to continue to analyze the impact and application of the security clauses and pursue a standard solution.

If you have any questions or require additional information regarding this waiver, please contact:

Janis Harrington, Assistant Director, Acquisitions Staff (202-616-6905) or by email at Janis.Harrington@usdoj.gov (*acquisition issues*);

Wolfgang Nickle, Chief, Policy, Acquisitions Staff (803-705-5653) or by email at Wolfgang.Nickle@usdoj.gov (*acquisition issues*);

Lynn Edelman, Civil Defensive Litigation Issues Coordinator, Office of Legal Programs Coordinator, Office of Legal Programs and Policy, (202-305-7403) or by email at Lynn.Edelman@usdoj.gov (*legal issues*); or,

Mark Fleshman, Chief Information Officer (202-616-6973) or by email at Mark.Fleshman@usdoj.gov (*technical issues*).

Attachment

Security of Systems and Data, Including Personally Identifiable Data of 25 or Fewer Individuals

a. Systems Security:

1. Keep the computer in a safe place, such as a locked office or other location with limited access, when not in use.
2. Mark any laptop with contact information in case of loss to facilitate its safe return.
3. Keep the operating system, security and application software used in connection with any computer updated on a regular basis.
4. Use anti-viral software and a host-based firewall mechanism.

b. Data Security:

Notify the primary or alternate contact with the USAO as soon as possible, but in no event more than 24 hours after discovery, of the loss of any computer or PII covered under the contract.

c. Personally Identifiable Information Notification

Notification to any individual whose personally identifiable information was, or is reasonably believed to have been, breached will be the responsibility of the Executive Office for United States Attorneys, consistent with the Department's Data Breach Notification Procedures.

d. Pass-through of Security Requirements to Subcontractors

The requirements set forth in Paragraphs a. through c. above, apply to all subcontractors who perform work in connection with this contract.

I certify that I have read and will adhere to the above security requirements.

Signature of Contractor or Authorized Representative

Date

Printed Name

2-23-10